DOCUMENT RESUME

ED 217 432 CS 206 952

AUTHOR Benjamin, Louise M.
TITLE Privacy Protection and Two-Way Cable Television: Report and Recommendations.
PUB DATE Jul 82
NOTE 23p.; Paper presented at the Annual Meeting of the Association for Education in Journalism (65th, Athens, OH, July 25-28, 1982).

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Cable Television; *Civil Liberties; *Federal Legislation; *Legal Problems; *Privacy; Technological Advancement; Television Research

ABSTRACT

Arguing that the threat to privacy in the new technological era of information processing and transmitting via cable television is a real one, this paper proposes that the threat can be minimized through effective legislation. The paper first looks at cable television privacy concerns and examines several studies concerning privacy, then reviews existing federal laws and court decisions concerning privacy in three areas applicable to two-way cable: (1) data gathering, storage, and dissemination; (2) disclosure of records held by third parties; and (3) eavesdropping or electronic surveillance. The paper also considers current state cable regulations and cable company self-regulatory practices regarding privacy. It then applies these studies, laws, and practices to formulating recommendations for future cable privacy legislation. The paper concludes with a list of 11 such recommendations that provide a guide for protecting cable subscribers' privacy. (FL)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED217432

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

This document has been reproduced as received from the person or organization originating it.
Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

PRIVACY PROTECTION

AND

TWO-WAY CABLE TELEVISION:

REPORT AND RECOMMENDATIONS

by
Louise M. Benjamin
School of Journalism and Mass Communication
University of Iowa
Iowa City, Iowa 52242

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Louise M. Benjamin

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

CS206152

Paper presented to the Special Session on Communication Technology and Policy at the Association for Education in Journalism Annual Convention in Athens, Ohio, July, 1982.

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. A man's answer to one question on one form becomes a little thread,...There are thus hundreds of little threads radiating from every man, millions of threads in all....They are not visible, they are not material, but every man is constantly aware of their existence....Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads... and for these people's authority.
>
> Alexander Solzhenitsyn
> Cancer Ward

INTRODUCTION

Like the man in this passage, Winston Smith knows about manipulation and authority. As a citizen of a totalitarian nation, he daily faces the technologies that thread together a pattern of his life. Acts considered dangerous to the Party have been recorded and Smith is under constant surveillance, even in his own apartment. Because of technological advances, Smith has no privacy -- that zone surrounding individuals which allows them to express innermost thoughts and which promotes human relationships and autonomous, free-thinking individuals necessary for self-government.[1] What Americans call "constitutional rights" are hollow legalisms in Oceania, Smith's homeland.

Lest one think Smith's plight in 1984 is far-fetched, a recent report by the Office of Technology Assessment states privacy rights are jeopardized because "computer technology through the 1980's will facilitate the collection of personal data, as well as make possible its instantaneous nationwide distribution."[2] As more transactions become computerized, "data that would normally not have been collected or retained will now be entered into computer systems and stored, thus becoming available to data collectors."[3]

It is feared some of this now-unrecorded information may be provided by cable television systems as their technology moves into interactive capabilities. Federal

Communications Commissioner Joseph Fogerty, stating the FCC's jurisdiction over cable is limited, asked Congress last fall to enact legislation to protect two-way cable subscribers[4]; the American Civil Liberties Union has begun a study to formulate recommendations for cable privacy protection. "The gist of the study will be aimed at two-way cable services, such as home banking, shopping, and other home-financing services. 'It's too easy to tap into these,'" according to Jay Miller, director of Illinois' ACLU.[5]

Potential abuses in cable's ability to collect, to process, and to disseminate information underlies these concerns. Such information-gathering poses problems ranging from unauthorized access to stored data to individuals' concerns about their right to control information stored about themselves. Several legislative attempts have been made to control computer information privacy in general[6]; at least one state legislature has been successful in enacting protections specifically for subscribers of cable television services.[7]

This paper examines the need for such legislation regarding two-way cable. First, it will look at cable television privacy concerns. Second, this paper will examine various federal studies concerning privacy and review existing federal laws and court decisions concerning privacy in three areas applicable to two-way cable: (1) data gathering, storage, and dissemination; (2) disclosure of records held by third parties; and (3) eaves dropping or electronic surveillance. Third, current state cable regulations and cable company self-regulatory practices will be examined. Fourth, this paper will apply these studies, laws, and self-regulatory practices to recommendations for future cable privacy legislation.

WHY WORRY ABOUT CABLE AND PRIVACY?

Cable telecommunications technologies are but one of the expanding information oriented services now being developed. Today, a vast variety of materials promised by cable companies in franchise bids can include banking and "tele-shopping" via cable, information retrieval services such as videotext and teletext, business-to-

business and business-to-home transactions, electronic mail services, home security devices, and custom-tailoring of commercials to fit specific buying habits of consumers. These require information exchange via cable and enable the monitoring of activities of individuals.

With current technologies such monitoring can now be done within seconds. The QUBE system computers in Columbus, Ohio, for example, can sweep subscriber homes every six seconds to determine who is watching what, using what service, or requesting special offers.[8] Out of necessity for business purposes, information used to bill for special services such as home security and pay movies is individually identifiable. This ability to pin-point specific subscribers has played to mixed reviews.

One cable subscriber, a diamond dealer, credits his cable home security service with saving his life. In January, 1981, he was shot by two men posing as customers. The men fled after his wife set off a cable security alarm that relayed a message for help.[9] The system's adult movie channel, however, has caused some subscribers to complain, not about morality but about the listing of viewing dates and times on monthly bills. The subscribers were homemakers who did not want their husbands to know they were watching "R" rated movies.[10] In other experimental situations in Texas and Indiana market-research firms monitor the grocery-store purchases of volunteer families and transmit custom-tailored commercials to the same families on an individualized basis via cable television. Marketing people are "elated" with the experiments while others such as the American Civil Liberties Union see the individualized commercials as an invasion of privacy.[11] When Cable News Network polled QUBE's subscribers asking if they were concerned about interactive cable's ability to invade privacy, seventy percent of those reponding said they were not worried.[12]

Others, though, are concerned. The ability of the identification of specific persons to threaten privacy was emphasized in three recent government reports.

The 1981 Office of Technology Assessment study[13] and two 1977 reports -- the Privacy Protection Study Commission[14] and the Report of the Commission on Federal Paperwork: Confidentiality and Privacy[15] -- state that with new technologies, centralization of records and integrated record-keeping systems threaten individual privacy. The manual systems used for centuries in information storage are being replaced by computerized systems which "bear no resemblance to earlier manual systems, but rather represent completely new approaches which could not be replicated in a manual environment."[16] With cable's ability for consolidating information services and its subsequent need for providing business records for such usage, privacy invasion becomes a more threatening possibility because records and information are stored in one central location -- the cable company's computer.

In 1975 John Eger, then acting director of the Office of Telecommunications Policy, warned in the forward to Kent Greenawalt's privacy report to OTP that Americans "face a future where information will play a central role, where control of information about a person could be tantamount to controlling that person."[17] In the report Greenawalt later links this sentiment directly to cable.[18]

Before the era of electronic devices, various barriers hampered the monitoring of a person's activities. In a statement during hearings in 1979 on privacy before the House Subcommittee of the Committee on Government, noted privacy scholar Alan Westin remarked during the last two decades

> ...microminiaturized bugs, television monitors, and devices capable of penetrating solid surfaces to listen or photograph dissolved the physical barriers of walls and doors that once assured privacy of speech and acts. Polygraph devices to measure emotional states and personality tests were increasingly being used to probe emotional and psychological states for purposes such as personnel selection. The development of electronic computers and long-distance communication networks now made it possible for large organizations to collect, store, and process far more information about an individual's life and transactions than was practical in the era of typewriter and file cabinet.[19]

A French scholar recently reminded conference attendees that if such storage and ready retrieval of information via wires and computers had been available in the 1930's and 1940's, Hitler "would have been able to round up the Jews at the push of a button."[20]

The necessary record-keeping involved in offering specialized cable services can also threaten privacy through a type of ex post facto surveillance. For example, transactions such as purchasing goods via cable and electronic funds transfers noting time of transactions could provide an invaluable resource for those wanting to determine an individual's preferences or to trace an individual's past actions. If these services are available chiefly through one source -- two-way cable -- the threat to privacy is more pronounced.

The possibility that any type of cable surveillance or monitoring may lead to self-censorship or manipulation is real. As stated in Technology and Privacy, Appendix 5 to the 1977 Privacy Protection Study Commission's report:

> The use of records to monitor the activities of individuals is obviously an area with profound public policy implications, regardless of the number in the group being monitored. As an issue, it goes to the heart of our basic constitutional liberties and cannot be ignored until the "crisis" stage is reached. While information technology will provide important new tools..., the possibility of a marked erosion of civil liberties must also be seriously considered.[21]

Since cable television is a growing part of these information technologies, legislation is needed to protect the civil liberties of individuals using two-way cable and to protect the records of cable subscribers.

STATUS OF PRIVACY PROTECTIONS: DATA GATHERING, STORAGE, AND DISSEMINATION

To protect an individual's privacy in this technological, information oriented environment, studies have been commissioned and legislation has been enacted during the past twelve years. Since 1970 Congress has passed four bills in response to

perceived potential misuse of personal information of the type which can now be processed by cable systems: the Fair Credit Reporting Act of 1970, the Privacy Act of 1974, the Family Education and Right to Privacy Act of 1974, and the Right to Financial Privacy Act of 1978. Of these, one -- the Fair Credit Reporting Act -- is aimed at private businesses; the others have been enacted to curb possible mishandling of information by government agencies and federally funded institutions. These four acts together with court decisions and federal eavesdropping laws act to protect the privacy of individuals from institutional invasions and government intrusions.[22]

The purpose of these acts may be summarized by the 1977 Congressional Privacy Protection Commission's statement that national policy must focus on three concurrent objectives: (1) minimize intrusiveness through creating a balance between what an individual is expected to divulge to a record-keeping organization and what he or she seeks in return; (2) maximize fairness by opening up record-keeping operations so recorded information is not a source of unfairness in decisions made about individuals; and (3) create legitimate, enforceable expectations of confidentiality.[23]

Ten principles emphasizing these objectives can be found throughout various reports on privacy and information protection. They have been incorporated into various information protection acts and pertain to both government and non-government, institutional record-keeping systems.

> (1) There should be no personal information system whose existence is secret.
>
> (2) Information should not be collected unless the need for it has been clearly established in advance.
>
> (3) Information should be appropriate and relevant to the purpose for which it has been collected.
>
> (4) Information should not be obtained by fraudulent or unfair means.
>
> (5) Information should not be used unless it is accurate and current.

> (6) There should be a prescribed procedure for an individual to know the existence of information stored about him, the purpose for which it has been recorded, particulars about its use and dissemination, and to examine that information.
>
> (7) There should be a clearly prescribed procedure for an individual to correct, erase, or amend inaccurate, obsolete, or irrelevant information.
>
> (8) Any organization collecting, maintaining, using, or disseminating personal information should assure its reliability and take precautions to prevent its misuse.
>
> (9) There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from being used for another purpose without his consent.
>
> (10) Federal, state and local government should not collect personal information except as expressly authorized by law.[24]

As stated earlier, these principles have been used in developing federal legislation to curb abuses regarding information practices in the private sector and in government.

The Fair Credit Reporting Act (FCRA) of 1970[25] attempts to halt possible abuse by credit reporting agencies without harming their ability to supply information for legitimate business needs. To date, it has been the only significant attempt to regulate the information practices of private business. It was enacted "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[26]

Basically, the act states credit agencies must adopt procedures to protect the confidentiality, accuracy, and use of information.[27] Under it, reports can be used only for specific purposes: (1) in response to a court order or to the written instructions by the person to whom it relates, (2) to determine eligibility for credit, insurance or employment or for a government-granted license or benefit in which an agency must consider the applicant's financial responsibility, or (3) to meet legitimate business needs in transactions involving the individual.[28]

Other sections of the act state the agency must notify the individual involved and furnish him or her with the name and address of the recipient of the report if the agency includes public information in its report which may cause an "adverse effect" -- denial of credit, insurance or employment or increased charges for credit or insurance.[29] In a similar fashion, if the user of the report takes an adverse action, he or she must notify the individual involved and provide him or her the name and address of the reporting agency.[30]

Under the act individuals may contest the accuracy and completeness of any information although the act suggests no specific procedure for initiating such action. To resolve a dispute, the agency must reinvestigate and delete inaccurate or unverified data; if the dispute is not resolved, the person has the right to file a statement of around 100 words which must be added to the file unless there are reasons to believe the statement frivilous or irrelevant.[31]

While the FCRA regulates private business, the Privacy Act of 1974 regulates the data collection and dissemination practices of various federal agencies.[32] An agency's records must be kept with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual."[33] The act states an individual has the right to inspect his or her records and, like the FCRA, gives an individual the opportunity to dispute and to correct a file. If a dispute is not resolved, the individual may add a "concise statement" of unspecified length to the file.[34] The act also requires agencies to keep an accurate account of a record's disclosure to those outside the agency unless that record is open to the public. These disclosures, too, must be available to affected individuals.[35] The act also provides civil relief for violations of its provisions, but individuals may recover damages only if the agency has acted intentionally or willfully.[36]

The Family Education and Right to Privacy Act provides a similar scheme of regulation for the information practices of federally funded educational institutions.[37]

For those institutions wishing to continue to benefit from federal funds, the release of personally identifiable school files without the consent of parents or of the students themselves, if they are over 18, is restricted.[38] The act also guarantees the parent or the student the right to see and to correct the student's file.[39]

The common threads of these three acts are individuals' access to records about themselves, the ability to dispute and to correct information contained therein, and the creation of individuals' expectations to privacy and confidentiality in use of their records. A fourth act -- the Right to Financial Privacy Act of 1978 -- seeks to control release of financial records held by third parties, financial institutions.

STATUS OF PRIVACY PROTECTIONS: DISCLOSURE OF RECORDS HELD BY THIRD PARTIES

Data collected and stored by third parties throws the ownership of such data into question.[40] In 1978 Congress passed the Right to Financial Privacy Act in response to the 1976 Supreme Court decision in United States v. Miller.[41] There the Court ruled bank depositors' records were not protected by the Fourth Admendment.

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government. The Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[42]

Thus, Congress passed the Right to Financial Privacy Act to protect the confidentiality of personal financial information held by financial institutions. The government, however, may obtain copies of such records through the use of subpoena and search warrant under certain conditions of notification of the customer involved.[43] The customer may challenge the government's actions.[44]

In its Miller ruling the Court was following the previous decisions regarding records[45] and re-emphasized them in two cases decided in 1979: Reporters' Committee

v. A.T. & T. and Smith v. Maryland.

In Reporters' Committee v. A.T. & T. the Supreme Court denied certiorari in a case involving release of journalists' toll-call records without providing prior notice to the journalists.[46] The District of Columbia Court of Appeals had ruled the Fourth Amendment protections against unreasonable search and seizure were not violated by the telephone company's policy of releasing records to law enforcement officials investigating a felony. The court recognized that an individual had a "zone of privacy," an area in which an individual could have reasonable expectations of privacy. So long as a person operated within this zone, the appeals courts said, his or her activities could be shielded from unreasonable government investigation.[47] But, the court added, "To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections, and, if the government is subsequently called upon to investigate his activities for possible violations of the law, it is free to seek out these third parties, to inspect their records, and to probe their recollections for evidence."[48]

In Smith v. Maryland the Court held that the installation and use of a "pen register" (a device used to record telephone numbers but which does not record conversation) was not a "search" within the meaning of the Fourth Amendment. Therefore, the Court ruled no warrant was necessary and the individual's "legitimate expectations" of privacy were not invaded.[49]

> ...we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills....it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[50]

These cases raise questions of production and ownership of records by third parties; such situations involving cable systems may have to be addressed by specific legislation as were financial records in the Miller case. Legislation covering development, use, and ownership of records kept by cable companies offering two-way services, however, should be enacted before problems arise.

STATUS OF PRIVACY PROTECTIONS: EAVESDROPPING OR ELECTRONIC SURVEILLANCE

The Smith v. Maryland case also underscores a third area of concern arising from the advent of two-way cable systems -- eavesdropping or electronic surveillance via cable. In Smith the Court stated the use of the pen register did not violate expectations of privacy because, in part, it was not a listening device which recorded a communication's content.[51] That type of surveillance is regulated primarily by two laws: Section 605 of the 1934 Communications Act[52] and Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[53] Section 605 is intended to regulate the conduct of common carrier personnel in their handling of wire and radio messages but has been interpreted to include any person handling such communication. Title III primarily regulates the conduct of government law enforcement officials in obtaining access to wire and oral communication but also applies to any person who "willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication."[54]

For the most part, these laws have failed to keep pace with communication technologies, according to John Metelski, former counsel for National Security Affairs of the Office of Telecommunication Policy. Metelski states these laws are limited in their application to new technologies and that as the "information society" becomes a reality, "the importance of laws which accurately and effectively satisfy the communications privacy expectations of individuals becomes essential if the classic balance between individual liberties and group (institutional or governmental) authority is to be preserved."[55]

This sentiment was emphasized in the Office of Technology Assessment study, Computer-Based National Information Systems. "The courts and Congress have been struggling for some time with interpretations of the Fourth Amendment in terms of wiretapping. Information systems that provide such services as electronic mail and electronic funds transfer will likely provoke similar debates in Congress."[56] Two-way cable is a part of these information systems; therefore, possible eavesdropping via cable becomes another facet of privacy protection to be specifically addressed in legislation.

CURRENT CABLE PRIVACY LAWS

Recognizing that subscribers' expectations of privacy protection must be met, states and municipalities are becoming involved in cable privacy legislation.[57] Illinois recently enacted what is the first state cable privacy law[58]; the new law prohibits communications companies, including two-way cable, from participating in any of four activities. Section 3 of the "Communications Consumer Privacy Act" reads that it shall be unlawful to:

> (1) install and use any equipment which would allow a communications company to visually observe or listen to what is occurring in an individual subscriber's household without the knowledge or permission of the subscriber
>
> (2) provide any person or public or private organization with a list containing the name of a subscriber, unless the communications company gives notice thereof to the subscriber
>
> (3) disclose the television viewing habits of any individual subscriber without the subscriber's consent; or
>
> (4) install or maintain a home-protection scanning device in a dwelling as part of a communication service without the express written consent of the occupant[59]

The act also calls for up to a $10,000 fine if violated.[60]

In mid-January, 1982, the attorney general for the state of New York asked the New York legislature to consider a cable privacy bill to protect subscribers' rights.[61]

Under the bill, written authorization for any interactive service (except for billing purposes or monitoring for system integrity) must be obtained in advance; individually identifiable information cannot be disclosed without written consent; upon written request, subscribers must be provided with individually identifiable information maintained by the cable system; if any information is disputed, the cable company must reinvestigate and correct any errors; if the dispute is not resolved, the subscriber may add a statement of not more than 500 words to his or her file. Any recipient of information must be supplied with a copy of such a statement. Finally, after in-house use of data is finished, the material must be destroyed.[62] The bill has been sent to both the New York house and senate.[63] Hearings were held in April and May and as of this writing, the proposed legislation awaits revision.[64]

The cable industry, in addition to government bodies, has expressed concern with the protection of subscribers' privacy.[65] Warner-Amex, operator of the Columbus, Ohio, interactive QUBE system, has recently adopted its own privacy code. Stating that "it is clearly possible to provide subscribers with the important benefits of interactive cable while at the same time guarding against real or perceived infringements of their individual rights," Warner-Amex has evolved a set of standards used to protect subscriber privacy.[66] The code puts into writing those procedures and policies followed by QUBE since to inception to protect subscriber privacy.[67] Under the code, cable communication information gathering functions shall be fully explained and adequate safeguards taken to ensure the physical security and confidentiality of subscriber information. Other provisions offer protections against release of individually identifiable information "in absence of legal compulsion, i.e. court order, subpoena" and state such information "will be retained for only as long as is reasonably necessary, e.g. to verify billings." Subscribers can examine and copy information developed by the cable company and, if a subscriber disputes the accuracy

of the information held, "Warner-Amex shall correct such records upon a reasonable showing by the subscriber that information contained therein is inaccurate." The code also states the cable company shall review and update the code to "keep current with technological changes" and that it shall comply "with applicable Federal, state, and local laws respecting subscriber privacy and shall adhere to applicable industry codes of conduct" regarding privacy.[68] To date, "there have been no real (subscriber) complaints" about privacy invasion; complaints about two-way services have involved billings for pay-per-view movies subscribers state they did not watch.[69] However, as information services increase, QUBE officials recognize that "the need to protect privacy is going to be great" and protection will involve a continuous re-evaluation of "privacy policies and practices to ensure their on-going effectiveness."[70]

The provisions outlined in the Warner-Amex code with those provisions contained in the Illinois statute and the proposed New York law can aid in developing recommendations for legislation regarding two-way cable privacy.

RECOMMENDATIONS FOR LEGISLATION

To balance the privacy needs of individuals with the legitimate needs of institutions or government for information, guidelines should be established to direct policy makers in the formation of interactive cable television privacy laws. The author makes the following recommendations which incorporate current laws, industry self-regulatory practices regarding information, and the provisions concerning information privacy outlined in various federal studies. Ideally, these recommendations should be adopted at the federal level to provide uniformity for the nation. However, with the current deregulatory mood toward cable, states, municipalities, and cable companies themselves will have the responsibility for insuring the privacy needs of individuals while maintaining legitimate informational needs of government and institutions. To balance these needs, the following eleven recommendations are made:

(1) Information may be collected via cable only when the legitimate need for it has been established. Such collection must be relevant to those needs and must be authorized in writing by the cable company and the cable subscriber.

(2) To prevent misuse of information by unauthorized individuals, a subscriber shall be informed in writing of the existence of individually identifiable information stored about him or her, the reasons the information has been recorded, and the extent of its use by and dissemination to others. Information used for one purpose shall not be used for other purposes without written consent from the subscriber.

(3) The cable company shall keep an accurate account of all occasions in which a record is disclosed and must furnish this to the subscriber before release occurs.

(4) The cable company shall make every effort to assure the reliability and accuracy of the information collected. The information shall be up-to-date.

(5) A subscriber shall be able to examine, correct, erase, or amend inaccurate, obsolete or irrelevant information through a prescribed procedure. The procedure shall involve a written request for review of all information held in the cable operator's files pertaining to the subscriber; the company shall provide assistance to the customer for review. Disputed information must be reinvestigated by the cable operator and, if the dispute is not resolved, the individual has the right to add a statement of up to 500 words to the file.

(6) The cable company shall not install or maintain any home-protection services or equipment which will allow the visual or aural observation of individual subscribers without the written consent of the subscriber and/or occupant.

(7) Lists of subscribers using or purchasing any service shall not be provided to any person or organization, public or private, without the subscriber's written consent in advance.

(8) Personal, subscriber-initiated transmissions (such as electronic mail) shall be encoded and decoded to protect the privacy of the transmissions.

(9) Recognizing that legitimate needs must be met in data processing and transmission, reports of individually identifiable information and viewing habits may be released to third parties only (a) in response to a court order ONLY after notification to the subscriber of such an order or (b) in response to the written instructions by the party to whom it relates.

(10) Upon completion of permissible uses, individually identifiable information stored by the cable company must be destroyed.

(11) Penalties should be provided for in cases involving violations of cable privacy. A violation, for example, shall be punishable by a fine not to exceed $10,000 for each violation.

CONCLUSION

In sum, the threat to privacy in the new technological era of information processing and transmitting via cable is a real one, but one which can be minimized by effective legislation. Conflicts can arise between data gathers/users and those about whom the data is gathered. Safeguards against illegitimate usages and access to cable-gathered data must be established. The recommendations contained in this paper provide a guide for protecting the cable subscriber's privacy. It is hoped laws based upon these guidelines will provide a realistic approach to the individual's right to control information about himself or herself. If such control is provided, an individual's hold on the threads of his or her life will be maintained and possible manipulation by others curtailed.

NOTES

1. See David L. Bazelon, "Probing Privacy" 12 Gonzaga Law Review 591 (1977). Alan Westin, Privacy and Freedom, New York: Atheneum, 1967. Kent Greenawalt, Legal Protections of Privacy: Final Report to the Office of Telecommunications Policy Washington, D.C.: U.S. Government Printing Office, 1975.

2. Computer-Based National Information Systems: Technology and Public Policy Issues, (Washington, D.C.: U.S. Government Printing Office, 1981), p. 76.

3. Ibid., p. 75

4. "FCC Commissioner Urges Cable Privacy Legislation," Multichannel News, September 28, 1981, p. 10.

5. "ACLU Study to Focus on Privacy in Cable," Multichannel News, October 12, 1981, p. 26.

6. See Julie Chinn, "Protecting Privacy from Government Invasion: Legislation at the Federal and State Levels," 8 Memphis State University Law Review 783 (1978); Gerald B. Cope, Jr. "Toward a Right of Privacy as a Matter of State Constitutional Law," 5 Florida State University Law Review 631 (1977); Hedy Gordon, "The Interface of Living Systems and Computers: The Legal Issues of Privacy," 2 Computer/Law Journal 877 (1980).

7. "Communications Consumer Privacy Act," Public Act 82-526, Illinois Legislative Service, 1981. Also see, "Illinois May Have First U.S. Cable-Privacy Law," Multichannel News, September 7, 1981, p. 4. and "Illinois Governor Signs Cable-Privacy Bill," Multichannel News, October 5, 1981, p. 2.

8. "The Television Explosion," NOVA, broadcast February 14, 1982, on the Public Broadcasting system. transcript "NOVA #906," p. 10.

9. John Andrew, "Home Security is a Cable TV, Industry Bets," Wall Street Journal, September 15, 1981, p. 25.

10. Margaret Yao, "Two-way Cable TV Disappoints Viewers in Columbus, Ohio, as Programming Lags," Wall Street Journal, September 30, 1981, p. 27.

11. Jeffery H. Birnbaum, "Admen Excited over New Marketing Tool, But Critics Contend It Smacks of '1984'," Wall Street Journal, September 25, 1981, p. 25.

12. "The Television Explosion," supra note 8, p. 14-15.

13. Computer-Based National Information Systems, supra note 2.

14. Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission. Washington, D.C.: U.S. Government Printing Office, 1977.

15. A Report of the Commission on Federal Paperwork: Confidentiality and Privacy. Washington, D.C.: U.S. Government Printing Office, 1977.

16. Kent Greenawalt, Legal Protections of Privacy: Final Report to the Office of Telecommunications Policy, (Washington, D.C.: U.S. Government Printing Office, 1975), p. 2. Also, see Arthur Miller's articles: "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society," 67 Michigan Law Review 1091 (1969) and "Computers, Data Banks and Individual Privacy: An Overview," 4 Columbia Human Rights Law Review 1 (1972).

17. Greenawalt, supra note 16, p. x.

18. Ibid., p. 13.

19. "Public Reaction to Privacy Issues," Hearings before the Subcommittee of the Committee on Government Operations, House of Representatives, 96th Congress 1st. session, p. 125-126.

20. Michael Pollen, "When the TV Set Turns Itself On," Channels, Feb/Mar 1982, p. 24-25.

21. Technology and Privacy, Appendix 5 to the Report of the Privacy Protection Study Commission, (Washington, D.C.: U.S. Government Printing Office, 1977), p. 33.

22. In non-governmental areas privacy invasion protections have grown largely from case law, state legislative efforts to curb abuse, and the Fair Credit Reporting Act. In 1960 William Prosser distinguished four tort actions in his oft-quoted article, "Privacy." [48 California Law Review 383 (1960)] These had developed in statutory law and court cases during the previous seventy years:

    (1) Intrusion upon the plaintiff's seclusion or solitude or into his private affairs
    (2) public disclosure of embarrassing private facts about the plaintiff
    (3) publicity which places the plaintiff in a false light
    (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness

Prosser's torts largely address actions by private interests such as the media and advertisers. Of the four, the first two -- "intrusion upon someone's seclusion" and "public disclosure of private facts" -- may be applied in the future as court decisions regarding cable television privacy evolve.

23. Personal Privacy in an Information Society, supra note 10, p. 14-15.

24. See Records, Computers and the Rights of Citizens, A Report of the HEW Secretary's Advisory Committee on Personal Data Systems, Washington, D.C.: U.S. Government Printing Office, 1973; "Recommendations of the Privacy Task Force," House Republican Research Committee, in Legislative History of the Privacy Act of 1974, 94th Congress 2nd session, p. 971-980; The Privacy Act of 1974, Public Law 93-579; "Federal Data Banks and Constitutional Rights," 93rd Congress 2nd session, (1974); A Report of the Commission on Federal Paperwork: Confidentiality and Privacy, Washington, D.C.: U.S. Government Printing Office, 1977. Also see Alan Westin and Michael Baker, Databanks in a Free Society: Computers, Record-keeping, and Privacy. New York: Quadrangle, 1972.

25. 15 U.S.C. §1681 (1970).

26. 15 U.S.C. §1681 (a)(4).

27. 15 U.S.C. §1681(b) and 15 U.S.C. §1681e(b).

28. 15 U.S.C. §1681b and 15 U.S.C. §1681e(a).

29. 15 U.S.C. §1681k.

30. 15 U.S.C. §1681m.

31. 15 U.S.C. §1681i.

32. 5 U.S.C. §552a (1976).

33. 5 U.S.C. §552a(e)(5).

34. 5 U.S.C. §552a(d).

35. 5 U.S.C. §552a(c).

36. 5 U.S.C. §552a(g).

37. 20 U.S.C. §1232g (1976).

38. 20 U.S.C. §1232g(b) and 20 U.S.C. §1232g(d).

39. 20 U.S.C. §1232g(a)

40. Computer-Based National Information Systems, supra note 2, p. 108.

41. 425 U.S. 435 (1976).

42. U.S. v. Miller, 425 U.S. 435, 443 (1976).

43. 12 U.S.C. §§3405-3409. These sections cover the use of subpoenas, summons, search warrants, formal written requests, and delayed notice sent to the customer involved.

44. 12 U.S.C. §3410. Customers may file motions to quash or applications to enjoin and may appeal decisions by courts.

45. Other cases involving records held by third parties include United States v. Lustig, 555 F.2d 737 (1977), cert. denied 434 U.S. 1045 (1978) [expectations of privacy extend to telephone conversations, not to records that conversations took place]; Couch v. United States, 409 U.S. 322 (1973)[taxpayer has no Fourth or Fifth Amendment right to contest a third party summons directed at taxpayer's accountant, even when it required production of taxpayer's own records]; Donaldson V. United States, 400 U.S. 517 (1971) [taxpayer has no standing to challenge IRS summons directed at employer's records relating to taxpayer]; First National Bank V. United States, 267 U.S. 576 (1925) [taxpayer has no Fourth Amendment basis for challenging internal revenue summons directed at third-party bank records relating to taxpayer]; Wilson v. United States, 221 U.S. 361 (1911) [corporation president has no Fourth Amendment interest in corporation's business records.]

46. 4 Med.L.Rptr. 1177 (D.C. Cir), cert. denied 4 Med.L.Rptr. 2536 (1979).

47. 4 Med.L.Rptr. 1177, 1183-1184 (1979).

48. 4 Med.L.Rptr. 1177, 1184 (1979).

49. Smith v. Maryland, 442 U.S. 735 (1979).

50. Smith v. Maryland, 442 U.S. 735, 742-743 (1979).

51. Smith v. Maryland, 442 U.S. 735, 741 (1979).

52. Communications Act of 1934, 47 U.S.C. §605.

53. Wire Interception and Interception of Oral Communications, 18 U.S.C. §§2510-2520.

54. 18 U.S.C. §2511.

55. John Metelski, "Achieving Communication Privacy through Revision of the Eavesdropping Laws," 30 Federal Communications Law Journal 135, 147 (1978).

56. Computer-Based National Information Systems, supra note 2, p. 110.

57. There is no "model" statute, however, suggested by the National Cable Television Association. Private communication with J. James McElveen, Director of Public Affairs, NCTA, March 15, 1982. One statute reads:

> It shall be unlawful for any firm, person, group, company, corporation, or government body to initiate or use any form, procedure, or device for monitoring or procuring information or data generated from or by cable subscribers' terminals, without prior written valid authorization from each subscriber so affected....

58. Private communication with J. James McElveen, supra note 52, and "Illinois May Have First U.S. Cable-Privacy Bill," Multichannel News, September 7, 1981 p. 4 and "Illinois Governor Signs Cable-Privacy Bill," Multichannel News, October 5, 1981, p. 2.

59. Communications Consumer Privacy Act, Public Act 82-526, Illinois Legislative Service, 1981.

60. Ibid., 4.

61. "Cable privacy concern in N.Y.," Broadcasting, January 18, 1982, p. 64.

62. Personal communication with Frank R. Fioramonti, assistant attorney general in charge, legislative bureau, State of New York, February 2, 1982, and March 26, 1982.

63. Bill now has sponsors and numbers -- S.8765 and A.11052, Senator Dale M. Volker and Assemblyman Melvin N. Zimmer respectively. Personal communication with Frank R. Fioramonti, March 26, 1982.

64. Personal communication with Kevin McGraw, State of New York, Assembly Governmental Operations Committee, June 23, 1982.

65. Personal communication with J. James McElveen, supra note 52.

66. Personal communication with Carol Lowe, community relations coordinator, QUBE-Warner-Amex Cable Communication Inc., March 16, 1982, and "Introduction" to "Code of Privacy Warner Amex Cable Communications," dated October 10, 1981.

67. Personal communication with Brian Beglane, community relations coordinator, QUBE-Warner-Amex Cable Communication Inc., June 24, 1982.

68. "Code of Privacy," supra note 66.

69. Personal Communication with Brian Beglane, supra note 67.

70. "Code of Privacy," supra note 66; Personal communication with Brian Beglane supra note 67; and Barbara Kransoff, "QUBE," Future Life, February, 1980, p. 38-39.